



US006285776B1

(12) **United States Patent**  
**Rhoads**(10) **Patent No.:** **US 6,285,776 B1**  
(45) **Date of Patent:** **Sep. 4, 2001**(54) **METHODS FOR IDENTIFYING EQUIPMENT  
USED IN COUNTERFEITING**0 581 317 A2 2/1994 (EP) ..... G07D/7/00  
0 590 884 A2 \* 4/1994 (EP) ..... H04N/1/00(75) Inventor: **Geoffrey B. Rhoads**, West Linn, OR  
(US)

(List continued on next page.)

(73) Assignee: **Digimarc Corporation**, Tualatin, OR  
(US)**OTHER PUBLICATIONS**( \* ) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 0 days.Gregory A. Baxes, *Digital image processing*, John Wiley &  
Sons, Inc. pp. 180-187, 1994.\*  
Pfitzmann, "Trials of Traced Traitors," Proc. 1st Int. Work-  
shop on Information Hiding, May/Jun. 1996, pp. 49-64.\*  
Nakamura et al., "A Unified Coding Method of Image and  
Text Data Using Discrete Orthogonal Transform," *Systems  
and Computers in Japan*, vol. 21, No. 3, 1990, pp. 87-92.\*

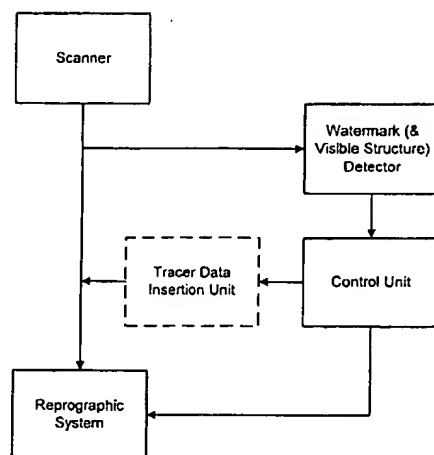
(List continued on next page.)

(21) Appl. No.: **09/293,602**(22) Filed: **Apr. 15, 1999***Primary Examiner*—Andrew W. Johns**Related U.S. Application Data**(74) *Attorney, Agent, or Firm*—William Y. Conwell;  
Digimarc Corporation(60) Division of application No. 09/074,034, filed on May 6,  
1998, which is a continuation-in-part of application No.  
08/438,159, filed on May 8, 1995, now Pat. No. 5,850,481,  
which is a continuation-in-part of application No. 08/327,  
426, filed on Oct. 21, 1994, now Pat. No. 5,768,426(60) Provisional application No. 60/082,228, filed on Apr. 16,  
1998.(51) **Int. Cl.<sup>7</sup>** ..... **H04K 1/00**(52) **U.S. Cl.** ..... **382/100; 380/51**(58) **Field of Search** ..... 382/100, 103,  
382/114, 116, 140; 705/27, 42, 43, 44,  
45, 51, 56, 58; 380/1, 3, 4, 6, 17, 20, 55,  
56(57) **ABSTRACT**(56) **References Cited****U.S. PATENT DOCUMENTS**3,918,567 11/1975 Kittredge ..... 197/1 R  
4,164,745 8/1979 Cielo et al. .... 346/140 R

(List continued on next page.)

**FOREIGN PATENT DOCUMENTS**2943436A1 5/1981 (DE) ..... G06K/19/06  
0234885B1 4/1991 (EP) ..... B41M/3/10  
0 551 016 A1 7/1993 (EP) .

Line art on a banknote or other security document is slightly changed to effect the encoding of plural-bit digital data (i.e. the banknote is digitally watermarked). When such a banknote is thereafter scanned, the resulting image data can be recognized as corresponding to a banknote by detection of the encoded data. (Alternatively, the image data can be recognized as corresponding to a banknote by machine detection of other forms of watermarking, or by reference to visible structures characteristic of banknotes.) In response to detection of a banknote, the detecting apparatus (e.g., a scanner, photocopier, or printer) can intervene by inserting forensic tracer data (e.g. steganographically encoded binary data) in the image data. The tracer data can memorialize the serial number of the machine that processed the banknote data and/or the date and time such processing occurred. To address privacy concerns, such tracer data is not normally inserted, but is so inserted only when the image data being processed is recognized as corresponding to a banknote. Any printed output from such image data will include the tracer data, permitting identification of equipment used in its reproduction.

**29 Claims, 3 Drawing Sheets**

## U.S. PATENT DOCUMENTS

4,297,729 10/1981 Steynor et al. .  
 4,571,489 2/1986 Watanabe ..... 235/379  
 4,588,212 5/1986 Castagnoli ..... 283/91  
 4,723,149 2/1988 Harada ..... 355/14 R  
 4,739,377 \* 4/1988 Allen ..... 355/133  
 4,943,093 7/1990 Melling et al. .... 283/83  
 5,091,966 2/1992 Bloomberg et al. .... 382/21  
 5,103,306 \* 4/1992 Weiman et al. .... 358/133  
 5,178,418 1/1993 Merry et al. .... 283/73  
 5,216,724 6/1993 Suzuki et al. .  
 5,257,119 \* 10/1993 Funada et al. .... 358/438  
 5,284,364 \* 2/1994 Jain ..... 283/87  
 5,305,199 4/1994 LoBiondo et al. .... 364/403  
 5,321,470 6/1994 Hasuo et al. .... 355/201  
 5,321,773 6/1994 Kopec et al. .... 382/30  
 5,336,871 \* 8/1994 Colgate, Jr. .... 235/380  
 5,374,976 12/1994 Spannenburg ..... 355/201  
 5,377,269 12/1994 Heptig et al. .... 380/25  
 5,390,003 2/1995 Yamaguchi et al. .... 355/201  
 5,390,259 2/1995 Withgott et al. .... 382/9  
 5,416,307 5/1995 Danek et al. .  
 5,424,807 6/1995 Ohmura .  
 5,426,710 6/1995 Suzuki et al. .  
 5,430,664 7/1995 Cargill et al. .... 364/550  
 5,434,427 7/1995 Crane et al. .... 250/556  
 5,437,897 8/1995 Tanaka et al. .... 428/29  
 5,453,968 9/1995 Veldhuis et al. .... 369/84  
 5,483,602 1/1996 Stenzel et al. .... 382/135  
 5,483,658 1/1996 Grube et al. .... 395/800  
 5,488,664 1/1996 Shamir ..... 380/54  
 5,502,576 \* 3/1996 Ramsay et al. .... 358/444  
 5,533,144 7/1996 Fan ..... 382/135  
 5,539,841 7/1996 Huttenlocher et al. .... 382/218  
 5,541,741 \* 7/1996 Suzuki ..... 358/450  
 5,550,932 8/1996 Blaylock et al. .... 382/139  
 5,557,742 9/1996 Smaha et al. .... 395/186  
 5,568,268 10/1996 Tsuji et al. .... 358/296  
 5,568,550 \* 10/1996 Ur ..... 380/3  
 5,572,010 11/1996 Petrie ..... 235/494  
 5,583,614 12/1996 Hasuo et al. .... 355/201  
 5,611,575 3/1997 Petrie ..... 283/67  
 5,613,004 3/1997 Cooperman et al. .  
 5,633,952 5/1997 Outa et al. .... 382/165  
 5,636,292 6/1997 Rhoads .  
 5,640,467 6/1997 Yamashita et al. .... 382/181  
 5,647,010 7/1997 Okubo et al. .  
 5,652,626 7/1997 Kawakami et al. .... 348/463  
 5,652,802 7/1997 Graves et al. .... 382/135  
 5,661,574 \* 8/1997 Kawana ..... 358/501  
 5,663,952 9/1997 Gentry, Jr. .... 370/252  
 5,671,277 9/1997 Ikenoue et al. .... 380/7  
 5,678,155 10/1997 Miyaza ..... 399/366  
 5,687,236 11/1997 Moskowitz et al. .  
 5,692,073 11/1997 Cass .  
 5,708,717 1/1998 Alasia .  
 5,710,636 1/1998 Curry ..... 358/298  
 5,710,834 1/1998 Rhoads .  
 5,721,788 2/1998 Powell et al. .... 382/100  
 5,727,092 3/1998 Sandford, II et al. .  
 5,735,547 4/1998 Morelle et al. .... 283/67  
 5,745,604 4/1998 Rhoads .  
 5,748,763 5/1998 Rhoads .  
 5,748,783 5/1998 Rhoads .  
 5,761,686 6/1998 Bloomberg .  
 5,772,249 6/1998 Guex et al. .... 283/93  
 5,790,693 8/1998 Graves et al. .

5,790,697 8/1998 Munro et al. .  
 5,796,824 8/1998 Hasebe et al. .... 380/4  
 5,822,448 10/1998 Graves et al. .  
 5,822,660 \* 10/1998 Wen ..... 399/194  
 5,825,892 10/1998 Braudaway et al. .... 380/51  
 5,838,814 11/1998 Moore ..... 382/115  
 5,841,886 11/1998 Rhoads ..... 382/115  
 5,843,564 12/1998 Gasper et al. .... 428/211  
 5,850,481 12/1998 Rhoads .  
 5,857,038 1/1999 Owada et al. .... 382/284  
 5,901,224 \* 5/1999 Hecht ..... 380/4  
 5,905,810 5/1999 Jones et al. .  
 5,949,903 9/1999 Outa et al. .  
 5,974,548 10/1999 Adams ..... 713/200  
 5,982,956 11/1999 Lahmi .  
 6,072,871 6/2000 Ur ..... 380/51  
 6,081,345 6/2000 Curry ..... 358/1.9

## FOREIGN PATENT DOCUMENTS

319 524 B1 6/1994 (EP) .  
 0 178 132 B2 8/1994 (EP) .  
 0 649 114 A2 4/1995 (EP) .  
 0 651 337 A1 5/1995 (EP) .  
 0 664 642 A2 7/1995 (EP) .  
 0 506 332 B1 12/1996 (EP) .  
 0 751 474 A2 1/1997 (EP) .  
 0 751 663 A2 1/1997 (EP) .  
 0 766 449 A2 4/1997 (EP) ..... H04N/1/00  
 0 789 270 A1 8/1997 (EP) ..... G03C/5/08  
 0789480A2 8/1997 (EP) ..... H04N/1/00  
 0 800 123 A2 10/1997 (EP) .  
 0 731 961 B1 5/1998 (EP) .  
 0 590 884 B1 6/1998 (EP) .  
 0 612 042 B1 6/1998 (EP) .  
 0 522 769 B1 9/1998 (EP) .  
 0 691 632 B1 10/1998 (EP) .  
 0 617 545 B1 1/1999 (EP) .  
 0 891 070 A1 1/1999 (EP) .  
 0 733 958 B1 5/1999 (EP) .  
 0 921 675 A2 6/1999 (EP) .  
 0 932 115 A2 7/1999 (EP) .  
 2 346 110 A 8/2000 (GB) ..... B41M/3/14  
 WO91/19614A1 12/1991 (WO) ..... B42D/15/10  
 WO95/04665A1 2/1995 (WO) ..... B44F/1/12  
 WO95/10813A1 4/1995 (WO) ..... G06F/15/403  
 WO95/14289A2 5/1995 (WO) ..... G06K/19/14  
 WO95/26274A1 10/1995 (WO) ..... B42D/15/10  
 WO 96/16381A1 5/1996 (WO) ..... G07D/7/00  
 WO 96/31049 10/1996 (WO) .  
 WO96/36163A2 11/1996 (WO) ..... H04N/1/32  
 WO97/43736 11/1997 (WO) ..... G06K/9/36  
 WO 99/17486 4/1999 (WO) .  
 WO 99/35819 7/1999 (WO) .  
 WO 99/36876 7/1999 (WO) .

## OTHER PUBLICATIONS

Szeoabsjum "A Signal Theoretic Method of Creating Forgery-Proof Documents for Automatic Verification," Proceedings 1979 Carnahan Conference on Crime Countermeasures, May 16, 1979, pp. 101-109.

Gruhl, "Information Hiding to Foil the Casual Counterfeiter", *Information Hiding*, 2d Int'l Workshop, pp. 1-15, Apr. 14, 1998.

Bender, "Techniques for Data Hiding," *SPIEvol.* 2420, Jan. 1995, pp. 164-173.

Gale, "Zero-Order Grating Microstructures," *Optical Document Security*, R.L. van Renesse, ed., Artech House, 1994, pp. 187-205.

\* cited by examiner

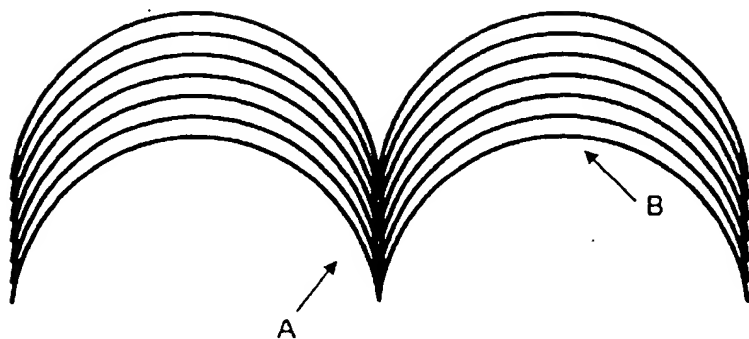


Fig. 1A  
(Prior art)

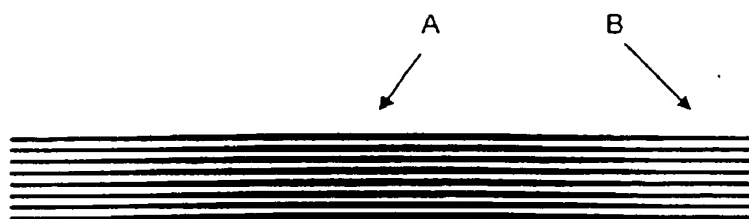


Fig. 1B  
(Prior art)

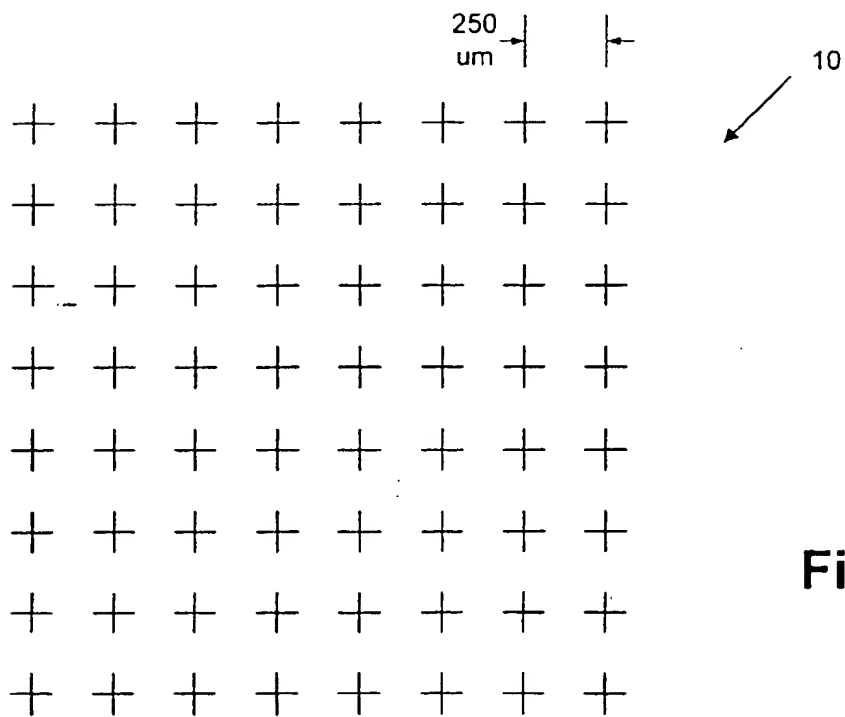
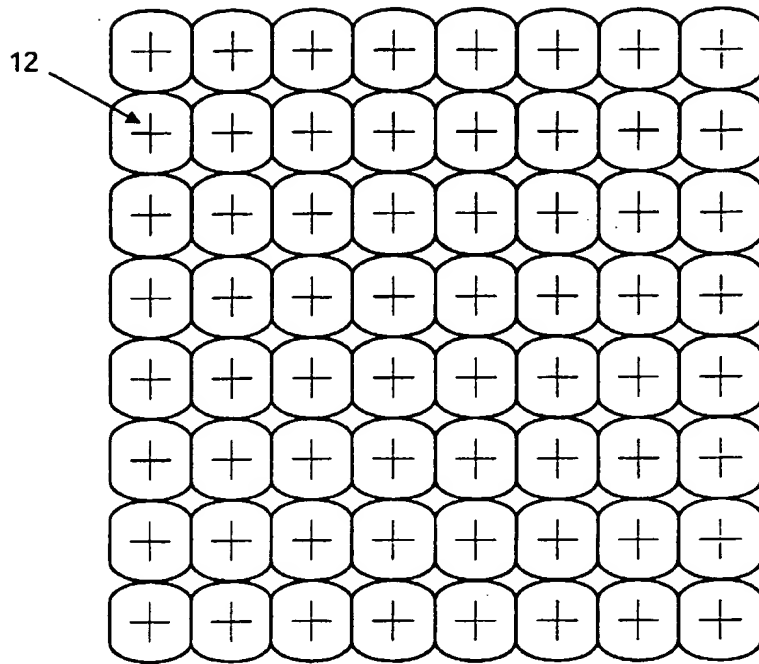
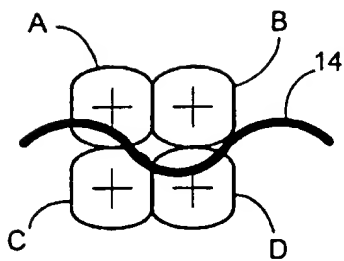


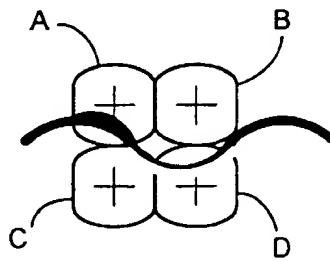
Fig. 2



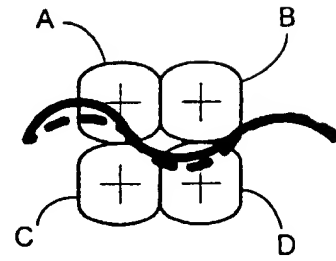
**Fig. 3**



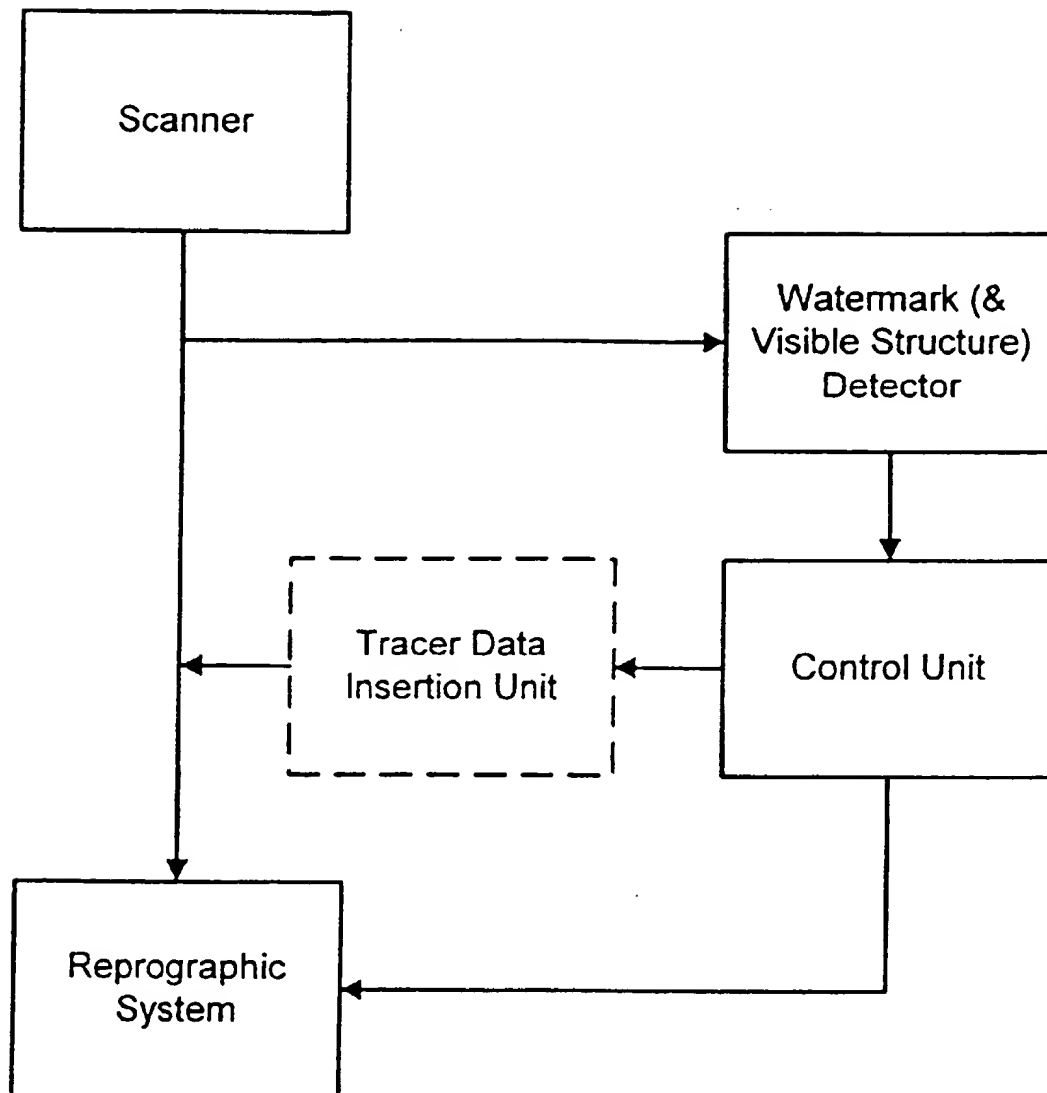
**Fig. 4**



**Fig. 5**



**Fig. 6**

**Fig. 7**

# METHODS FOR IDENTIFYING EQUIPMENT USED IN COUNTERFEITING

## RELATED APPLICATION DATA

This application is a divisional application of copending utility application Ser. No. 09/074,034, filed May 6, 1998, which is a continuation-in-part of application Ser. No. 08/438,159, filed May 8, 1995 (now U.S. Pat. No. 5,850,481), and provisional application Ser. No. 60/082,228, filed Apr. 16, 1998. Application Ser. No. 08/438,159 is a continuation-in-part of application Ser. No. 08/327,426, filed Oct. 21, 1994 (now U.S. Pat. No. 5,768,426).

(The specification of application Ser. No. 08/438,159 is substantially identical to that of applicant's issued U.S. Pat. Nos. 5,636,292, 5,710,834, 5,748,763, 5,748,783. The specification of application 60/082,228 is attached hereto as Appendix A.)

A sibling divisional application, Ser. No. 09/293,601, is filed herewith and is entitled Methods and Devices For Recognizing Banknotes and Responding Accordingly.

The subject matter of this application is also related to that of the present assignee's other pending applications, namely Ser. No. 08/508,083 (now U.S. Pat. No. 5,841,978), Ser. No. 08/534,005 (now U.S. Pat. No. 5,832,119), Ser. No. 08/637,531 (now U.S. Pat. No. 5,822,436), Ser. No. 08/649,419 (now U.S. Pat. No. 5,862,260), Ser. No. 08/746,613 (now U.S. Pat. No. 6,122,403), Ser. No. 08/951,858 (now U.S. Pat. No. 6,026,193), and Ser. No. 08/969,072 (now U.S. Pat. No. 5,809,160), and the allowed applications referenced below.

## FIELD OF THE INVENTION

The present invention relates to embedding binary data in image data so as to identify, e.g., equipment with which the image data was processed. The invention finds particular application in deterring counterfeiting of banknotes.

## BACKGROUND AND SUMMARY OF THE INVENTION

Watermarking is a quickly growing field of endeavor, with several different approaches. The present assignee's work is reflected in U.S. Pat. Nos. 5,710,834, 5,636,292, 5,721,788, 5,748,763, 5,748,783, and 5,745,604, in allowed U.S. applications Ser. No. 08/327,426 (now U.S. Pat. No. 5,768,426), Ser. No. 08/508,083 (now U.S. Pat. No. 5,841,978), Ser. No. 08/1438,159 (now U.S. Pat. No. 5,850,481), and in laid-open PCT application WO97/43736. Other work is illustrated by U.S. Pat. Nos. 5,734,752, 5,646,997, 5,659,726, 5,664,018, 5,671,277, 5,687,191, 5,687,236, 5,689,587, 5,568,570, 5,572,247, 5,574,962, 5,579,124, 5,581,500, 5,613,004, 5,629,770, 5,461,426, 5,743,631, 5,488,664, 5,530,759, 5,539,735, 4,943,973, 5,337,361, 5,404,160, 5,404,377, 5,315,098, 5,319,735, 5,337,362, 4,972,471, 5,161,210, 5,243,423, 5,091,966, 5,113,437, 4,939,515, 5,374,976, 4,855,827, 4,876,617, 4,939,515, 4,963,998, 4,969,041, and published foreign applications WO 98/02864, EP 822,550, WO 97/39410, WO 96/36163, GB 2,196,167, EP 777,197, EP 736,860, EP 705,025, EP 766,468, EP 782,322, WO 95/20291, WO 96/26494, WO 96/36935, WO 96/42151, WO 97/22206, WO 97/26733. Some of the foregoing patents relate to visible watermarking techniques. Other visible watermarking techniques (e.g. data glyphs) are described in U.S. Pat. Nos. 5,706,364, 5,689,620, 5,684,885, 5,680,223, 5,668,636, 5,640,647, 5,594,809.

Most of the work in watermarking, however, is not in the patent literature but rather in published research. In addition

to the patentees of the foregoing patents, some of the other workers in this field (whose watermark-related writings can be found by an author search in the INSPEC database) include I. Pitas, Eckhard Koch, Jian Zhao, Norishige Morimoto, Laurence Boney, Kinco Matsui, A. Z. Tirkel, Fred Mintzer, B. Macq, Ahmed H. Tewfik, Frederic Jordan, Naohisa Komatsu, and Lawrence O'Gorman.

The artisan is assumed to be familiar with the foregoing prior art.

In the following disclosure it should be understood that references to watermarking encompass not only the assignee's watermarking technology, but can likewise be practiced with any other watermarking technology, such as those indicated above.

Watermarking can be applied to myriad forms of information. The present disclosure focuses on its applications to line art imagery, of the sort typically employed in banknotes, travelers checks, passports, stock certificates, and the like (hereafter collectively referred to as "banknotes"). However, it should be recognized that the principles discussed below can also be applied outside this particular field.

Most of the prior art in image watermarking has focused on pixelated imagery (e.g. bit-mapped images, JPEG/MPEG imagery, VGA/SVGA display devices, etc.). In most watermarking techniques, the luminance or color values of component pixels are slightly changed to effect subliminal encoding of binary data through the image. (This encoding can be done directly in the pixel domain, or in another domain, such as the DCT domain.) In some systems, isolated pixels are changed in accordance with one or more bits of the binary data; in others, plural domain-related groupings of pixels (e.g. locally adjoining, or corresponding to a given DCT component) are so changed. In all cases, however, pixels have served as the ultimate carriers of the embedded data.

While pixelated imagery is a relatively recent development, line art goes back centuries. One familiar example is U.S. paper currency. On the one dollar banknote, for example, line art is used in several different ways. One is to form intricate webbing patterns around the margin of the note (generally comprised of light lines on dark background). Another is to form grayscale imagery, such as the portrait of George Washington (generally comprised of dark lines on a light background).

In an illustrative embodiment of the present invention, the line art on a banknote or other security document is slightly changed to effect the encoding of plural-bit digital data (i.e. the banknote is digitally watermarked). When such a banknote is thereafter scanned, the resulting image data can be recognized as corresponding to a banknote by detection of the encoded data. (Alternatively, the image data can be recognized as corresponding to a banknote by machine detection of other forms of watermarking, or by reference to visible structures characteristic of banknotes.)

In response to detection of a banknote, the detecting apparatus (e.g., a scanner, photocopier, or printer) can intervene by inserting forensic tracer data (e.g. steganographically encoded binary data) in the image data. The tracer data can memorialize the serial number of the machine that processed the banknote data and/or the date and time such processing occurred. To address privacy concerns, such tracer data is not normally inserted, but is so inserted only when the image data being processed is recognized as corresponding to a banknote. Any printed output from such image data will include the tracer data, permitting identification of equipment used in its reproduction.

3

The foregoing features and advantages of the invention will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

### BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. 1A and 1B show prior art techniques for achieving grayscale effects using line art.

FIG. 2 shows a virtual array of grid points that can be imposed on an image according to one embodiment of the present invention.

FIG. 3 shows a virtual array of regions that can be imposed on an image according to the FIG. 2 embodiment.

FIG. 4 shows an excerpt of FIG. 3 with a line from a line art image passing therethrough.

FIG. 5 shows changes to the width of the line of FIG. 3 to effect watermark encoding according to one embodiment of the present invention.

FIG. 6 shows changes to the position of the line of FIG. 3 to effect watermark encoding according to another embodiment of the present invention.

FIG. 7 is a block diagram of a photocopier according to another embodiment of the invention.

### DETAILED DESCRIPTION

Referring to FIG. 2, an illustrative form of the invention employs a grid 10 of imaginary reference points arrayed over a line art image. The spacing between points is 250  $\mu$ m in the illustrated arrangement, but greater or lesser spacings can of course be used.

Associated with each grid point is a surrounding region 12, shown in FIG. 3. As described below, the luminosity (or reflectance) of each of these regions 12 is slightly changed to effect the subliminal encoding of binary data.

Region 12 can take various shapes; the illustrated rounded-rectangular shape is representative only. (The illustrated shape has the advantage of encompassing a fairly large area while introducing fewer visual artifacts than, e.g., square regions.) In other embodiments, squares, rectangles, circles, ellipses, etc., can alternatively be employed.

FIG. 4 is a magnified view of an excerpt of FIG. 3, showing a line 14 passing through the grid of points. The width of the line, of course, depends on the particular image of which it is a part. The illustrated line is about 25  $\mu$ m in width; greater or lesser widths can naturally be used.

In a first embodiment of the invention, shown in FIG. 5, the width of the line is controllably varied so as to change the luminosity of the regions through which it passes. To increase the luminosity (or reflectance), the line is made narrower (i.e. less ink in the region). To decrease the luminosity, the line is made wider (i.e. more ink).

Whether the luminance in a given region should be increased or decreased depends on the particular watermarking algorithm used. Any algorithm can be used, by changing the luminosity of regions 12 as the algorithm would otherwise change the luminance or colors of pixels in a pixelated image.

In an exemplary algorithm, the binary data is represented as a sequence of -1s and 1s, instead of 0s and 1s. (The binary data can comprise a single datum, but more typically comprises several. In an illustrative embodiment, the data comprises 100 bits.)

Each element of the binary data sequence is then multiplied by a corresponding element of a pseudo-random

4

number sequence, comprised of -1s and 1s, to yield an intermediate data signal. Each element of this intermediate data signal is mapped to a corresponding sub-part of the image, such as a region 12. The image in (and optionally around) this region is analyzed to determine its relative capability to conceal embedded data, and a corresponding scale factor is produced. Exemplary scale factors may range from 0 to 3. The scale factor for the region is then multiplied by the element of the intermediate data signal mapped to the region in order to yield a "tweak" value for the region. In the illustrated case, the resulting tweaks can range from -3 to 3. The luminosity of the region is then adjusted in accordance with the tweak value. A tweak value of -3 may correspond to a -5% change in luminosity; -2 may correspond to -2% change; 1 may correspond to -1% change; 0 may correspond to no change; 1 may correspond to +1% change; 2 may correspond to +2% change, and 3 may correspond to +5% change. (This example follows the basic techniques described in the Real Time Encoder embodiment disclosed in U.S. Pat. No. 5,710,834.)

In FIG. 5, the watermarking algorithm determined that the luminance of region A should be reduced by a certain percentage, while the luminance of regions C and D should be increased by certain percentages.

In region A, the luminance is reduced by increasing the line width. In region D, the luminance is increased by reducing the line width; similarly in region C (but to a lesser extent).

No line passes through region B, so there is no opportunity to change the region's luminance. This is not fatal to the method, however, since the watermarking algorithm redundantly encodes each bit of data in subparts spaced throughout the line art image.

The changes to line widths in regions A and D of FIG. 5 are exaggerated for purposes of illustration. While the illustrated variance is possible, most implementations will modulate the line width 3-50% (increase or decrease).

(Many watermarking algorithms routinely operate within a signal margin of about +/-1% changes in luminosity to effect encoding. That is, the "noise" added by the encoding amounts to just 1% or so of the underlying signal. Lines typically don't occupy the full area of a region, so a 10% change to line width may only effect a 1% change to region luminosity, etc. Banknotes are different from photographs in that the art need not convey photorealism. Thus, banknotes can be encoded with higher energy than is used in watermarking photographs, provided the result is still aesthetically satisfactory. To illustrate, localized luminance changes on the order of 10% are possible in banknotes, while such a level of watermark energy in photographs would generally be considered unacceptable. In some contexts, localized luminance changes of 20, 30, 50 or even 100% are acceptable.)

In the illustrated embodiment, the change to line width is a function solely of the tweak to be applied to a single region. Thus, if a line passes through any part of a region to which a tweak of 2% is to be applied, the line width in that region is changed to effect the 2% luminance difference. In variant embodiments, the change in line width is a function of the line's position in the region. In particular, the change in line width is a function of the distance between the region's center grid point and the line's closest approach to that point. If the line passes through the grid point, the full 2% change is effected. At successively greater distances, successively less change is applied. The manner in which the magnitude of the tweak changes as a function of line



5

position within the region can be determined by applying one of various interpolation algorithms, such as the bi-linear, bi-cubic, cubic splines, custom curve, etc.

In other variant embodiments, the change in line width in a given region is a weighted function of the tweaks for adjoining or surrounding regions. Thus, the line width in one region may be increased or decreased in accordance with a tweak value corresponding to one or more adjoining regions.

Combinations of the foregoing embodiments can also be employed.

In the foregoing embodiments, it is sometimes necessary to trade-off the tweak values of adjoining regions. For example, a line may pass along a border between regions, or pass through the point equidistant from four grid points ("equidistant zones"). In such cases, the line may be subject to conflicting tweak values—one region may want to increase the line width, while another may want to decrease the line width. (Or both may want to increase the line width, but differing amounts.) Similarly in cases where the line does not pass through an equidistant zone, but the change in line width is a function of a neighborhood of regions whose tweaks are of different values. Again, known interpolation functions can be employed to determine the weight to be given the tweak from each region in determining what change is to be made to the line width in any given region.

In the exemplary watermarking algorithm, the average change in luminosity across the image is zero, so no generalized lightening or darkening of the image is apparent. The localized changes in luminosity are so minute in magnitude, and localized in position, that they are essentially invisible (e.g. inconspicuous/subliminal) to human viewers.

An alternative embodiment is shown in FIG. 6, in which line position is changed rather than line width.

In FIG. 6 the original position of the line is shown in dashed form, and the changed position of the line is shown in solid form. To decrease a region's luminosity, the line is moved slightly closer to the center of the grid point; to increase a region's luminosity, the line is moved slightly away. Thus, in region A, the line is moved towards the center grid point, while in region D it is moved away.

It will be noted that the line on the left edge of region A does not return to its nominal (dashed) position as it exits the region. This is because the region to the left of region A also is to have decreased luminosity. Where possible, it is generally preferable not to return a line to its nominal position, but instead permit shifted lines to remain shifted as they enter adjoining regions. So doing permits a greater net line movement within a region, increasing the embedded signal level.

Again, the line shifts in FIG. 6 are somewhat exaggerated. More typical line shifts are on the order of 3–50  $\mu\text{m}$ .

One way to think of the FIG. 6 embodiment is to employ a magnetism analogy. The grid point in the center of each region can be thought of as a magnet. It either attracts or repels lines. A tweak value of  $-3$ , for example, may correspond to a strong-valued attraction force; a tweak value of  $+2$  may correspond to a middle-valued repulsion force, etc. In FIG. 6, the grid point in region A exhibits an attraction force (i.e. a negative tweak value), and the grid point in region D exhibits a repulsion force (e.g. a positive tweak value).

The magnetic analogy is useful because the magnetic effect exerted on a line depends on the distance between the line and the grid point. Thus, a line passing near a grid point is shifted more in position than a line near the periphery of the region.

6

Each of the variants discussed above in connection with FIG. 5 is likewise applicable to FIG. 6.

Combinations of the embodiments of FIGS. 5 and 6 can of course be used, resulting in increased watermark energy, better signal-to-noise ratio and, in many cases, less noticeable changes.

In still a further embodiment, the luminance in each region is changed while leaving the line unchanged. This can be effected by sprinkling tiny dots of ink in the otherwise-vacant parts of the region. In high quality printing, of the type used with banknotes, droplets on the order of 3  $\mu\text{m}$  in diameter can be deposited. (Still larger droplets are still beyond the perception threshold for most viewers.) Speckling a region with such droplets (either in a regular array, or random, or according to a desired profile such as Gaussian), can readily effect a 1% or so change in luminosity. (Usually dark droplets are added to a region, effecting a decrease in luminosity. Increases in luminosity can be effected by speckling with a light colored ink, or by forming light voids in line art otherwise present in a region.)

In a variant of the speckling technique, very thin mesh lines can be inserted in the artwork—again to slightly change the luminance of one or more regions.

Although not previously mentioned, it is contemplated that the banknote will include some manner of calibration information to facilitate registration of the image for decoding. This calibration information can be steganographic or overt. Several techniques for steganographically embedding calibration information are disclosed in my prior patents and applications. Other techniques can be found in others of the cited work.

To decode watermark data, the encoded line art image must be converted into electronic form for analysis. This conversion is typically performed by a scanner.

Scanners are well known, so a detailed description is not provided here. Suffice it to say that scanners conventionally employ a line of closely spaced photodetector cells that produce signals related to the amount of the light reflected from successive swaths of the image. Most inexpensive consumer scanners have a resolution of 300 dots per inch (dpi), or a center to center spacing of component photodetectors of about 84  $\mu\text{m}$ . Higher quality scanners of the sort found in most professional imaging equipment and photocopiers have resolutions of 600 dpi (42  $\mu\text{m}$ ), 1200 dpi (21  $\mu\text{m}$ ), or better.

Taking the example of a 300 dpi scanner (84  $\mu\text{m}$  photodetector spacing), each 250  $\mu\text{m}$  region 12 on the banknote will correspond to about a 3x3 array of photodetector samples. Naturally, only in rare instances will a given region be physically registered with the scanner so that nine photodetector samples capture the luminance in that region, and nothing else. More commonly, the line art is skewed with respect to the scanner photodetectors, or is longitudinally misaligned (i.e. some photodetectors image sub-parts of two adjoining regions). However, since the scanner oversamples the regions, the luminance of each region can unambiguously be determined.

In one embodiment, the scanned data from the line art is collected in a two dimensional array and processed—according to one of the techniques disclosed in my prior patents and applications—to detect the embedded calibration information. The array is then processed to effect a virtual re-registration of the image data. A software program then analyzes the statistics of the re-registered data (using the techniques disclosed in my prior writings) to extract the bits of the embedded data.

(Again, the reference to my earlier watermark decoding techniques is exemplary only. Once scanning begins and the data is available in pixel form, it is straightforward to apply any other watermark decoding technique to extract a correspondingly-encoded watermark.)

In a variant embodiment, the scanned data is not assembled in a complete array prior to the processing. Instead, it is processed in real-time, as it is generated, in order to detect embedded watermark data without delay. (Depending on the parameters of the scanner, it may be necessary to scan a half-inch or so of the line art image before the statistics of the resulting data unambiguously indicate the presence of a watermark.)

In accordance with another aspect of the invention, various hardware devices are provided with the capability to recognize embedded watermark data in any line art images they process, and to respond accordingly.

One example is a color photocopier. Such devices employ a color scanner to generate sampled (pixel) data corresponding to an input media (e.g. a dollar bill). If watermark data associated with a banknote is detected, the photocopier can take one or more steps.

One option is simply to interrupt copying, and display a message reminding the operator that it is illegal to reproduce currency.

Another option is to dial a remote service and report the attempted reproduction of a banknote. Photocopiers with dial-out capabilities are known in the art (e.g. U.S. Pat. No. 5,305,199) and are readily adapted to this purpose. The remote service can be an independent service, or can be a government agency.

Yet another option is to permit the copying, but to insert forensic tracer data in the resultant copy. This tracer data can take various forms. Steganographically encoded binary data is one example. An example is shown in U.S. Pat. No. 5,568,268. The tracer data can memorialize the serial number of the machine that made the copy and/or the date and time the copy was made. To address privacy concerns, such tracer data is not normally inserted in photocopied output, but is so inserted only when the subject being photocopied is detected as being a banknote. (Such an arrangement is shown in FIG. 7.)

Desirably, the scan data is analyzed on a line-by-line basis in order to identify illicit photocopying with a minimum of delay. If a banknote is scanned, one or more lines of scanner output data may be provided to the photocopier's reprographic unit before the banknote detection decision has been made. In this case the photocopy will have two regions: a first region that is not tracer-marked, and a second, subsequent region in which the tracer data has been inserted.

Photocopiers with other means to detect not-to-be-copied documents are known in the art, and employ various response strategies. Examples are detailed in U.S. Pat. Nos. 5,583,614, 4,723,149, 5,633,952, 5,640,467, and 5,424,807.

Another hardware device that can employ the foregoing principles is a standalone scanner. A programmed processor (or dedicated hardware) inside the scanner analyzes the data being generated by the device, and responds accordingly.

Yet another hardware device that can employ the foregoing principles is a printer. A processor inside the device analyzes graphical image data to be printed, looking for watermarks associated with banknotes.

For both the scanner and printer devices, response strategies can include disabling operation, or inserting tracer information. (Such devices typically do not have dial-out capabilities.)

Again, it is desirable to process the scanner or printer data as it becomes available, so as to detect any banknote processing with a minimum of delay. Again, there will be some lag time before a detection decision is made.

Accordingly, the scanner or printer output will be comprised of two parts, one without the tracer data, and another with the tracer data.

Banknotes presently include various visible structures that can be used as aids in banknote detection (e.g. the seal of the issuing central bank, and various geometrical markings). In accordance with a further aspect of the present invention, a banknote is analyzed by an integrated system that considers both the visible structures and watermark-embedded data.

Visible banknote structures can be sensed using known pattern recognition techniques. Examples of such techniques are disclosed in U.S. Pat. Nos. 5,321,773, 5,390,259, 5,533,144, 5,539,841, 5,583,614, 5,633,952, 4,723,149 and 5,424,807 and laid-open foreign application EP 766,449.

In photocopiers (and the like) equipped to detect both visible and watermarked banknote markings, the detection of either causes one or more of the above-noted banknote responses to be initiated.

Again, scanners and printers can be equipped with a similar capability-analyzing the data for either of these banknote hallmarks. If either is detected, the software (or hardware) responds accordingly.

Identification of banknotes by watermark data provides an important advantage over recognition by visible structures—it cannot so easily be defeated. A banknote can be doctored (e.g. by white-out, scissors, or less crude techniques) to remove/obliterate the visible structures. Such a document can then be freely copied on either a visible structure-sensing photocopier or scanner/printer installation. The removed visible structure can then be added in via a second printing/photocopying operation. If the printer is not equipped with banknote-disabling capabilities, image-editing tools can be used to insert visible structures back into image data sets scanned from such doctored bills, and the complete bill freely printed. By additionally including embedded watermark data in the banknote, and sensing same, such ruses will not succeed.

(A similar ruse is to scan a banknote image on a non-banknote-sensing scanner. The resulting image set can then be edited by conventional image editing tools to remove/obliterate the visible structures. Such a data set can then be printed—even on a printer/photocopier that examines such data for the presence of visible structures. Again, the missing visible structures can be inserted by a subsequent printing/photocopying operation.)

Desirably, the visible structure detector and the watermark detector are integrated together as a single hardware and/or software tool. This arrangement provides various economies, e.g., in interfacing with the scanner, manipulating pixel data sets for pattern recognition and watermark extraction, electronically re-registering the image to facilitate pattern recognition/watermark extraction, issuing control signals (e.g. disabling) signals to the photocopier/scanner, etc.

(To provide a comprehensive disclosure without unduly lengthening the following specification, applicants incorporate by reference the patent documents cited above.)

From the foregoing, it will be recognized that embodiments according to the present invention allow banknotes to be recognized based on optical scan data, and responsive actions taken, thereby reducing the risk of counterfeiting.

Having described and illustrated the principles of my invention with reference to several illustrative embodiments, it will be recognized that these embodiments are exemplary only and should not be taken as limiting the scope of my invention. Guided by the foregoing teachings, it should be apparent that other watermarking, decoding, and anti-counterfeiting technologies can be substituted for, and/or combined with, the elements detailed above to yield similar effects.

While the invention has been described with reference to embodiments employing regular rectangular arrays of grid points, those skilled in the art will recognize that other arrays of points—neither rectangular nor regular—can alternatively be used.

While the invention has been described with reference to embodiments that scale the embedded energy in accordance with local image characteristics, in other embodiments a manually crafted energy profile can be implemented. That is, a mask defining embedded signal magnitudes at different parts of the image can be manually devised, and employed to tailor the change in luminance in each region.

In view of the many possible embodiments to which the principles of the invention may be put, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of my invention. Rather, I claim as my invention all such embodiments as may come within the scope and spirit of the following claims and equivalents thereto.

#### APPENDIX A

##### Specification of 60/082,228

##### Watermarking Methods, Apparatuses, and Applications

(To provide a comprehensive disclosure without unduly lengthening the following specification, applicants incorporate by reference the cited patent documents.)

Watermarking is a quickly growing field of endeavor, with several different approaches. The present assignee's work is reflected in U.S. Pat. Nos. 5,710,834, 5,636,292, 5,721,788, allowed U.S. applications Ser. Nos. 08/327,426, 08/598,083, 08/436,134 (to issue as U.S. Pat. No. 5,748,763), Ser. No. 08/436,102 (to issue as U.S. Pat. No. 5,748,783), and Ser. No. 08/614,521 (to issue as U.S. Pat. No. 5,745,604), and laid-open PCT application WO97/43736. Other work is illustrated by U.S. Pat. Nos. 5,734,752, 5,646,997, 5,659,726, 5,664,018, 5,671,277, 5,687,191, 5,687,236, 5,689,587, 5,568,570, 5,572,247, 5,574,962, 5,579,124, 5,581,500, 5,613,004, 5,629,770, 5,461,426, 5,743,631, 5,488,664, 5,530,759, 5,539,735, 4,943,973, 5,337,361, 5,404,160, 5,404,377, 5,315,098, 5,319,735, 5,337,362, 4,972,471, 5,161,210, 5,243,423, 5,091,966, 5,113,437, 4,939,515, 5,374,976, 4,855,827, 4,876,617, 4,939,515, 4,963,998, 4,969,041, and published foreign applications WO 98/02864, EP 822,550, WO 97/39410, WO 96/36163, GB 2,196,167, EP 777,197, EP 736,860, EP 705,025, EP 766,468, EP 782,322, WO 95/20291, WO 96/26494, WO 96/36935, WO 96/42151, WO 97/22206, WO 97/26733. Some of the foregoing patents relate to visible watermarking techniques. Other visible watermarking techniques (e.g. data glyphs) are described in U.S. Pat. Nos. 5,706,364, 5,689,620, 5,684,885, 5,680,223, 5,668,636, 5,640,647, 5,594,809.

Most of the work in watermarking, however, is not in the patent literature but rather in published research. In addition to the patentees of the foregoing patents, some of the other workers in this field (whose watermark-related writings can be found by an author search in the INSPEC database) include I. Pitas, Eckhard Koch, Jian Zhao, Norishige

Morimoto, Laurence Boney, Kineo Matsui, A. Z. Tirkel, Fred Mintzer, B. Macq, Ahmed H. Tewfik, Frederic Jordan, Naohisa Komatsu, and Lawrence O'Gorman.

The artisan is assumed to be familiar with the foregoing prior art.

In the following disclosure it should be understood that references to watermarking encompass not only the assignee's watermarking technology, but can likewise be practiced with any other watermarking technology, such as those indicated above.

Watermarking can be applied to myriad forms of information. These include imagery (including video) and audio—whether represented in digital form (e.g. an image comprised of pixels, digital video, etc.), or in an analog representation (e.g. non-sampled music, printed imagery, banknotes, etc.) Watermarking can be applied to digital content (e.g. imagery, audio) either before or after compression. Watermarking can also be used in various "description" or "synthesis" language representations of content, such as Structured Audio, Csound, NetSound, SNHC Audio and the like (c.f. <http://sound.media.mit.edu/mpeg4/>) by specifying synthesis commands that generate watermark data as well as the intended audio signal. Watermarking can also be applied to ordinary media, whether or not it conveys information. Examples include paper, plastics, laminates, paper/film emulsions, etc. A watermark can embed a single bit of information, or any number of bits.

The physical manifestation of watermarked information most commonly takes the form of altered signal values, such as slightly changed pixel values, picture luminance, picture colors, DCT coefficients, instantaneous audio amplitudes, etc. However, a watermark can also be manifested in other ways, such as changes in the surface microtopology of a medium, localized chemical changes (e.g. in photographic emulsions), localized variations in optical density, localized changes in luminescence, etc. Watermarks can also be optically implemented in holograms and conventional paper watermarks.

One improvement to existing technology is to employ established web crawler services (e.g. Alta Vista, Excite, or Inktomi) to search for watermarked content (on the Web, in internet news groups, BBS systems, on-line systems, etc.) in addition to their usual data collecting/indexing operations. Such crawlers can download files that may have embedded watermarks (e.g. \*.JPG, \*.WAV, etc.) for later analysis. These files can be processed, as described below, in real time. More commonly, such files are queued and processed by a computer distinct from the crawler computer. Instead of performing watermark-read operations on each such file, a screening technique can be employed to identify those most likely to be conveying watermark data. One such technique is to perform a DCT operation on an image, and look for spectral coefficients associated with certain watermarking techniques (e.g. coefficients associated with an inclined embedded subliminal grid). To decode spread-spectrum based watermarks, the analyzing computer requires access to the noise signal used to spread the data signal. In one embodiment, interested parties submit their noise/key signals to the crawler service so as to enable their marked content to be located. The crawler service maintains such information in confidence, and uses different noise signals in decoding an image (image is used herein as a convenient shorthand for imagery, video, and audio) until watermarked data is found (if present). This allows the use of web crawlers to locate content with privately-coded watermarks, instead of just publicly-coded watermarks as is presently the case. The queuing of content data for analysis provides

certain opportunities for computational shortcuts. For example, like-sized images (e.g. 256x256 pixels) can be tiled into a larger image, and examined as a unit for the presence of watermark data. If the decoding technique (or the optional pre-screening technique) employs a DCT transform or the like, the block size of the transform can be tailored to correspond to the tile size (or some integral fraction thereof). Blocks indicated as likely having watermarks can then be subjected to a full read operation. If the queued data is sorted by file name, file size, or checksum, duplicate files can be identified. Once such duplicates are identified, the analysis computer need consider only one instance of the file. If watermark data is decoded from such a file, the content provider can be informed of each URL at which copies of the file were found.

Some commentators have observed that web crawler-based searches for watermarked images can be defeated by breaking a watermarked image into sub-blocks (tiles). HTML instructions, or the like, cause the sub-blocks to be presented in tiled fashion, recreating the complete image. However, due to the small size of the component sub-blocks, watermark reading is not reliably accomplished.

This attack is overcome by instructing the web-crawler to collect the display instructions (e.g. HTML) by which image files are positioned for display on a web page, in addition to the image files themselves. Before files collected from a web page are scrutinized for watermarks, they can be concatenated in the arrangement specified by the display instructions. By this arrangement, the tiles are reassembled, and the watermark data can be reliably recovered.

Another such postulated attack against web crawler detection of image watermarks is to scramble the image (and thus the watermark) in a file, and employ a Java applet or the like to unscramble the image prior to viewing. Existing web crawlers inspect the file as they find it, so the watermark is not detected. However, just as the Java descrambling applet can be invoked when a user wishes access to a file, the same applet can similarly be employed in a web crawler to overcome such attempted circumvention of watermark detection.

Although "content" can be located and indexed by various web crawlers, the contents of the "content" are unknown. A \*.JPG file, for example, may include pornography, a photo of a sunset, etc.

Watermarks can be used to indelibly associate meta-data within content (as opposed to stored in a data structure that forms another part of the object, as is conventionally done with meta-data). The watermark can include text saying "sunset" or the like. More compact information representations can alternatively be employed (e.g. coded references). Still further, the watermark can include (or consist entirely of) a Unique ID (UID) that serves as an index (key) into a network-connected remote database containing the meta data descriptors. By such arrangements, web crawlers and the like can extract and index the meta-data descriptor tags, allowing searches to be conducted based on semantic descriptions of the file contents, rather than just by file name.

Existing watermarks commonly embed information serving to communicate copyright information. Some systems embed text identifying the copyright holder. Others embed a UID which is used as an index into a database where the name of the copyright owner, and associated information, is stored.

Looking ahead, watermarks should serve more than as silent copyright notices. One option is to use watermarks to embed "intelligence" in content. One form of intelligence is knowing its "home." "Home" can be the URL of a site with

which the content is associated. A photograph of a car, for example, can be watermarked with data identifying the web site of an auto-dealer that published the image. Wherever the image goes, it serves as a link back to the original disseminator. The same technique can be applied to corporate logos. Wherever they are copied on the internet, a suitably-equipped browser or the like can decode the data and link back to the corporation's home page. (Decoding may be effected by positioning the cursor over the logo and pressing the right-mouse button, which opens a window of options—one of which is Decode Watermark.)

To reduce the data load of the watermark, the intelligence need not be wholly encoded in the content's watermark. Instead, the watermark can again provide a UID—this time identifying a remote database record where the URL of the car dealer, etc., can be retrieved. In this manner, images and the like become marketing agents—linking consumers with vendors (with some visual salesmanship thrown in). In contrast to the copyright paradigm, in which dissemination of imagery was an evil sought to be tracked and stopped, dissemination of the imagery can now be treated as a selling opportunity. A watermarked image becomes a portal to a commercial transaction.

(Using an intermediate database between a watermarked content file and its ultimate home (i.e. indirect linking) serves an important advantage: it allows the disseminator to change the "home" simply by updating a record in the database. Thus, for example, if one company is acquired by another, the former company's smart images can be made to point to the new company's home web page by updating a database record. In contrast, if the old company's home URL is hard-coded (i.e. watermarked) in the object, it may point to a URL that eventually is abandoned. In this sense, the intermediate database serves as a switchboard that couples the file to its current home.

The foregoing techniques are not limited to digital content files. The same approach is equally applicable with printed imagery, etc. A printed catalog, for example, can include a picture illustrating a jacket. Embedded in the picture is watermarked data. This data can be extracted by a simple hand-scanner/decoder device using straightforward scanning and decoding techniques (e.g. those known to artisans in those fields). In watermark-reading applications employing hand-scanners and the like, it is important that the watermark decoder be robust to rotation of the image, since the catalog photo will likely be scanned off-axis. One option is to encode subliminal graticules (e.g. visualization synchronization codes) in the catalog photo so that the set of image data can be post-processed to restore it to proper alignment prior to decoding.

The scanner/decoder device can be coupled to a modem-equipped computer, a telephone, or any other communications device. In the former instance, the device provides URL data to the computer's web browser, linking the browser to the catalog vendor's order page. (The device need not include its own watermark decoder; this task can be performed by the computer.) The vendor's order page can detail the size and color options of the jacket, inventory availability, and solicit ordering instructions (credit card number, delivery options, etc.)—as is conventionally done with on-line merchants. Such a device connected to a telephone can dial the catalog vendor's toll-free automated order-taking telephone number (known, e.g., from data encoded in the watermark), and identify the jacket to the order center. Voice prompts can then solicit the customer's choice of size, color, and delivery options, which are input by Touch Tone instructions, or by voiced words (using known voice recognition software at the vendor facility).

In such applications, the watermark may be conceptualized as an invisible bar code employed in a purchase transaction. Here, as elsewhere, the watermark can serve as a seamless interface bridging the print and digital worlds.

Another way of providing content with intelligence is to use the watermark to provide Java or ActiveX code. The code can be embedded in the content, or can be stored remotely and linked to the content. When the watermarked object is activated, the code can be executed (either automatically, or at the option of the user). This code can perform virtually any function. One is to "phone home"—initiating a browser and linking to the object's home. The object can then relay any manner of data to its home. This data can specify some attribute of the data, or its use. The code can also prevent accessing the underlying content until permission is received. An example is a digital movie that, when double-clicked, automatically executes a watermark-embedded Java applet which links through a browser to the movie's distributor. The user is then prompted to input a credit card number. After the number has been verified and a charge made, the applet releases the content of the file to the computer's viewer for viewing of the movie. Support for these operations is desirably provided via the computer's operating system, or plug-in software.

Such arrangements can also be used to collect user-provided demographic information when smart image content is accessed by the consumer of the content. The demographic information can be written to a remote database and can be used for market research, customization of information about the content provided to the consumer, sales opportunities, advertising, etc.

In audio and video and the like, watermarks can serve to convey related information, such as links to WWW fan sites, actor biographies, advertising for marketing tie-ins (T-shirts, CDs, concert tickets). In such applications, it is desirable (but not necessary) to display on the user interface (e.g. screen) a small logo to signal the presence of additional information. When the consumer selects the logo via some selection device (mouse, remote control button, etc.), the information is revealed to the consumer, who can then interact with it.

Much has been written (and patented) on the topic of asset rights management. Sample patent documents include U.S. Pat. No. 5,715,403, 5,638,443, 5,634,012, 5,629,980. Again, much of the technical work is memorialized in journal articles, which can be identified by searching for relevant company names and trademarks such as IBM's Cryptolope system, Portland Software's ZipLock system, the Rights Exchange service by Softbank Net Solutions, and the Digi-Box system from InterTrust Technologies.

An exemplary asset management system makes content available (e.g. from a web server, or on a new computer's hard disk) in encrypted form. Associated with the encrypted content is data identifying the content (e.g. a preview) and data specifying various rights associated with the content. If a user wants to make fuller use of the content, the user provides a charge authorization (e.g. a credit card) to the distributor, who then provides a decryption key, allowing access to the content. (Such systems are often realized using object-based technology. In such systems, the content is commonly said to be distributed in a "secure container.")

Desirably, the content should be marked personalized/serialized) so that any illicit use of the content (after decryption) can be tracked. This marking can be performed with watermarking, which assures that the mark travels with the content wherever—and in whatever form—it may go. The watermarking can be effected by the distributor—prior

to dissemination of the encrypted object—such as by encoding a UID that is associated in a database with that particular container. When access rights are granted to that container, the database record can be updated to reflect the purchaser, the purchase date, the rights granted, etc. An alternative is to include a watermark encoder in the software tool used to access (e.g. decrypt) the content. Such an encoder can embed watermark data in the content as it is released from the secure container, before it is provided to the user. The embedded data can include a UID, as described above. This UID can be assigned by the distributor prior to disseminating the container. Alternatively, the UID can be a data string not known or created until access rights have been granted. In addition to the UID, the watermark can include other data not known to the distributor, e.g. information specific to the time(s) and manner(s) of accessing the content.

In other systems, access rights systems can be realized with watermarks without containers etc. Full resolution images, for example, can be freely available on the web. If a user wishes to incorporate the imagery into a web page or a magazine, the user can interrogate the imagery as to its terms and conditions of use. This may entail linking to a web site specified by the embedded watermark (directly, or through an intermediate database), which specifies the desired information. The user can then arrange the necessary payment, and use the image knowing that the necessary rights have been secured.

As noted, digital watermarks can also be realized using conventional (e.g. paper) watermarking technologies. Known techniques for watermarking media (e.g. paper, plastic, polymer) are disclosed in U.S. Pat. Nos. 5,536,468, 5,275,870, 4,760,239, 4,256,652, 4,370,200, and 3,985,927 and can be adapted to display of a visual watermark instead of a logo or the like. Note that some forms of traditional watermarks which are designed to be viewed with transmissive light can also show up as low level signals in reflective light, as is typically used in scanners. Transmissive illumination detection systems can also be employed to detect such watermarks, using optoelectronic traditional-watermark detection technologies known in the art.

As also noted, digital watermarks can be realized as part of optical holograms. Known techniques for producing and securely mounting holograms are disclosed in U.S. Pat. Nos. 5,319,475, 5,694,229, 5,492,370, 5,483,363, 5,658,411 and 5,310,222. To watermark a hologram, the watermark can be represented in the image or data model from which the holographic diffraction grating is produced. In one embodiment, the hologram is produced as before, and displays an object or symbol. The watermark markings appear in the background of the image so that they can be detected from all viewing angles. In this context, it is not critical that the watermark representation be essentially imperceptible to the viewer. If desired, a fairly visible noise-like pattern can be used without impairing the use to which the hologram is put.

Digital watermarks can also be employed in conjunction with labels and tags. In addition to conventional label/tag printing processes, other techniques—tailored to security—can also be employed. Known techniques useful in producing security labels/tags are disclosed in U.S. Pat. Nos. 5,665,194, 5,732,979, 5,651,615, and 4,268,983. The imperceptibility of watermarked data, and the ease of machine decoding, are some of the benefits associated with watermarked tags/labels. Additionally, the cost is far less than many related technologies (e.g. holograms). Watermarks in this application can be used to authenticate the originality of a product label, either to the merchant or to the consumer of

15

the associated product, using a simple scanner device, thereby reducing the rate of counterfeit product sales.

Recent advances in color printing technology have greatly increased the level of casual counterfeiting. High quality scanners are now readily available to many computer users, with 300 dpi scanners available for under \$100, and 600 dpi scanners available for marginally more. Similarly, photographic quality color ink-jet printers are commonly available from Hewlett-Packard Co., Epson, etc. for under \$300.

Watermarks in banknotes and other security documents (passports, stock certificates, checks, etc.—all collectively referred to as banknotes herein) offer great promise to reduce such counterfeiting, as discussed morefully below. Additionally, watermarks provide a high-confidence technique for banknote authentication. One product enabled by this increased confidence is automatic teller machines that accept, as well as dispense, cash. The machine is provided with known optical scanning technology to produce digital data corresponding to the face(s) of the bill. This image set is then analyzed to extract the watermark data. In watermarking technologies that require knowledge of a code signal for decoding (e.g. noise modulation signal, crypto key, spreading signal, etc.), a bill may be watermarked in accordance with several such codes. Some of these codes are public—permitting their reading by conventional machines. Others are private, and are reserved for use by government agencies and the like. (C.f. public and private codes in the present assignee's issued patents)

Banknotes presently include certain markings which can be used as an aid in note authentication. Well known visible structures are added to banknotes to facilitate visual authentication and machine detection. An example is the seal of the issuing central bank. Others are geometrical markings. Desirably, a note is examined by an integrated detection system, for both such visible structures as well as the present watermark-embedded data, to determine authenticity.

The visible structures can be sensed using known pattern recognition techniques. Examples of such techniques are disclosed in U.S. Pat. Nos. 5,321,773, 5,390,259, 5,533,144, 5,539,841, 5,583,614, 5,633,952, 4,723,149 and 5,424,807 and laid-open foreign application EP 766,449. The embedded watermark data can be recovered using the scanning/analysis techniques disclosed in the cited patents and publications.

To reduce counterfeiting, it is desirable that document-reproducing technologies recognize banknotes and refuse to reproduce same. A photocopier, for example, can sense the presence of either a visible structure \*or\* embedded banknote watermark data, and disable copying if either is present. Scanners and printers can be equipped with a similar capability—analyzing the data scanned or to be printed for either of these banknote hallmarks. If either is detected, the software (or hardware) disables further operation.

The watermark detection criteria provides an important advantage not otherwise available. An original bill can be doctored (e.g. by white-out, scissors, or less crude techniques) to remove/obliterate the visible structures. Such a document can then be freely copied on either a visible structure-sensing photocopier or scanner/printer installation. The removed visible structure can then be added in via a second printing/photocopying operation. If the printer is not equipped with banknote-disabling capabilities, image-editing tools can be used to insert visible structures back into image data sets scanned from such doctored bills, and the complete bill freely printed. By additionally including embedded watermark data in the banknote, and sensing same, such ruses will not succeed.

16

(A similar ruse is to scan a banknote image on a non-banknote-sensing scanner. The resulting image set can then be edited by conventional image editing tools to remove/obliterate the visible structures. Such a data set can then be printed—even on a printer/photocopier that examines such data for the presence of visible structures. Again, the missing visible structures can be inserted by a subsequent printing/photocopying operation.)

Desirably, the visible structure detector and the watermark detector are integrated together as a single hardware and/or software tool. This arrangement provides various economies, e.g., in interfacing with the scanner, manipulating pixel data sets for pattern recognition and watermark extraction, electronically re-registering the image to facilitate pattern recognition/watermark extraction, issuing control signals (e.g. disabling) signals to the photocopier/scanner, etc.

A related principle is to insert an imperceptible watermark having a UID into all documents printed with a printer, scanned with a scanner, or reproduced by a photocopier. The UID is associated with the particular printer/photocopier/scanner in a registry database maintained by the products' manufacturers. The manufacturer can also enter in this database the name of the distributor to whom the product was initially shipped. Still further, the owner's name and address can be added to the database when the machine is registered for warranty service. While not preventing use of such machines in counterfeiting, the embedded UID facilitates identifying the machine that generated a counterfeit banknote. (This is an application in which a private watermark might best be used.)

While the foregoing applications disabled potential counterfeiting operations upon the detection of \*either\* a visible structure or watermarked data, in other applications, both criteria must be met before a banknote is recognized as genuine. Such applications typically involve the receipt or acceptance of banknotes, e.g. by ATMs as discussed above.

The foregoing principles (employing just watermark data, or in conjunction with visible indicia) can likewise be used to prevent counterfeiting of tags and labels (e.g. the fake labels and tags commonly used in pirating Levis brand jeans, Microsoft software, etc.)

The reader may first assume that banknote watermarking is effected by slight alterations to the ink color/density/distribution, etc. on the paper. This is one approach. Another is to watermark the underlying medium (whether paper, polymer, etc.) with a watermark. This can be done by changing the microtopology of the medium (a la mini-Braille) to manifest the watermark data. Another option is to employ a laminate on or within the banknote, where the laminate has the watermarking manifested thereon/therein. the laminate can be textured (as above), or its optical transmissivity can vary in accordance with a noise-like pattern that is the watermark, or a chemical property can similarly vary.

Another option is to print at least part of a watermark using photoluminescent ink. This allows, e.g., a merchant presented with a banknote, to quickly verify the presence of \*some\* watermark-like indicia in/on the bill even without resort to a scanner and computer analysis (e.g. by examining under a black light). Such photoluminescent ink can also print human-readable indicia on the bill, such as the denomination of a banknote. (Since ink-jet printers and other common mass-printing technologies employ cyan/magenta/yellow/black to form colors, they can produce only a limited spectrum of colors. Photoluminescent colors are outside their capabilities. Fluorescent colors—such as the yellow,



17

pink and green dyes used in highlighting markers—can similarly be used and have the advantage of being visible without a black light.)

An improvement to existing encoding techniques is to add an iterative assessment of the robustness of the mark with a corresponding adjustment in a re-watermarking operation. Especially when encoding multiple bit watermarks, the characteristics of the underlying content may result in some bits being more robustly (e.g. strongly) encoded than others. In an illustrative technique employing this improvement, a watermark is first embedded in an object. Next, a trial decoding operation is performed. A confidence measure (e.g. signal-to-noise ratio) associated with each bit detected in the decoding operation is then assessed. The bits that appear weakly encoded are identified, and corresponding changes are made to the watermarking parameters to bring up the relative strengths of these bits. The object is then watermarked anew, with the changed parameters. This process can be repeated, as needed, until all of the bits comprising the encoded data are approximately equally detectable from the encoded object, or meet some predetermined signal-to-noise ratio threshold.

The foregoing applications, and others, can generally benefit by multiple watermarks. For example, an object (physical or data) can be marked once in the spatial domain, and a second time in the spatial frequency domain. (It should be understood that any change in one domain has repercussions in the other. Here we reference the domain in which the change is directly effected.)

Another option is to mark an object with watermarks of two different levels of robustness, or strength. The more robust watermark withstands various types of corruption, and is detectable in the object even after multiple generations of intervening distortion. The less robust watermark can be made frail enough to fail with the first distortion of the object. In a banknote, for example, the less robust watermark serves as an authentication mark. Any scanning and reprinting operation will cause it to become unreadable. Both the robust and the frail watermarks should be present in an authentic banknote; only the former watermark will be present in a counterfeit.

Still another form of multiple-watermarking is with content that is compressed. The content can be watermarked once (or more) in an uncompressed state. Then, after compression, a further watermark (or watermarks) can be applied.

Still another advantage from multiple watermarks is protection against sleuthing. If one of the watermarks is found and cracked, the other watermark(s) will still be present and serve to identify the object.

The foregoing discussion has addressed various technological fixes to many different problems. Exemplary solutions have been detailed above. Others will be apparent to the artisan by applying common knowledge to extrapolate from the solutions provided above.

For example, the technology and solutions disclosed herein have made use of elements and techniques known from the cited references. Other elements and techniques from the cited references can similarly be combined to yield further implementations within the scope of the present invention. Thus, for example, holograms with watermark data can be employed in banknotes, single-bit watermarking can commonly be substituted for multi-bit watermarking, technology described as using imperceptible watermarks can alternatively be practiced using visible watermarks (glyphs, etc.), techniques described as applied to images can likewise be applied to video and audio, local scaling of

18

watermark energy can be provided to enhance watermark signal-to-noise ratio without increasing human perceptibility, various filtering operations can be employed to serve the functions explained in the prior art, watermarks can include subliminal gratitudes to aid in image re-registration, encoding may proceed at the granularity of a single pixel (or DCT coefficient), or may similarly treat adjoining groups of pixels (or DCT coefficients), the encoding can be optimized to withstand expected forms of content corruption. Etc., etc., etc. Thus, the exemplary embodiments are only selected samples of the solutions available by combining the teachings referenced above. The other solutions necessarily are not exhaustively described herein, but are fairly within the understanding of an artisan given the foregoing disclosure and familiarity with the cited art.

I claim:

1. A method of image processing, comprising:

providing image data corresponding to an optically scanned document to a processing apparatus; and digitally watermarking the image data with a machine readable, image-adapted, steganographic digital watermark representing plural bit binary data, said digital watermark serving to mark the image data as having been processed on said apparatus;

wherein said image data thereafter carries said digital watermark embedded therein, permitting the apparatus on which said image data was processed to be identified;

the method further including watermarking the image data only if the image data is recognized to correspond to a security document.

2. The method of claim 1 which includes recognizing a security document by reference to visible structures expressed in said image data.

3. The method of claim 1 which includes recognizing a security document by reference to a steganographic digital watermark already encoded in said image data and detectable in image data produced by visible light scanning of said document.

4. The method of claim 1 which includes decoding a watermark in the input document to recognize the input document as a security document.

5. A method of image processing, comprising:

providing image data corresponding to an optically scanned document to a processing apparatus; and digitally watermarking the image data with a machine readable, image-adapted, steganographic digital watermark representing plural bit binary data, said digital watermark serving to mark the image data as having been processed on said apparatus;

wherein said image data thereafter carries said digital watermark embedded therein, permitting the apparatus on which said image data was processed to be identified, and wherein said plural bit binary data is encoded redundantly through the image data, rather than each bit being encoded in a single localized region only.

6. A method of image processing, comprising:

providing image data corresponding to an optically scanned document to a processing apparatus; and digitally watermarking the image data with a machine readable, image-adapted, steganographic digital watermark representing plural bit binary data, said digital watermark serving to mark the image data as having been processed on said apparatus;

wherein said image data thereafter carries said digital watermark embedded therein, permitting the apparatus

19

on which said image data was processed to be identified, and wherein the digital watermarking makes use of a discrete cosine transform.

7. A method of image processing, comprising:

providing image data corresponding to an optically scanned document to a processing apparatus; and  
digitally watermarking the image data with a machine readable, image-adapted, steganographic digital watermark representing plural bit binary data, said digital watermark serving to mark the image data as having been processed on said apparatus;

wherein said image data thereafter carries said digital watermark embedded therein, permitting the apparatus on which said image data was processed to be identified;

wherein the digital watermarking includes encoding a calibration signal with the plural bit digital data so as to facilitate decoding of the watermark, and in which the calibration signal is adapted to facilitate decoding of the watermark notwithstanding rotation of the image data.

8. A method of image processing, comprising:

providing image data corresponding to an optically scanned document to a processing apparatus; and  
digitally watermarking the image data with a machine readable, image-adapted, steganographic digital watermark representing plural bit binary data, said digital watermark serving to mark the image data as having been processed on said apparatus;

wherein said image data thereafter carries said digital watermark embedded therein, permitting the apparatus on which said image data was processed to be identified;

the method also including digitally watermarking the image data with two different digital watermarks.

9. The method of claim 8 in which the two different digital watermarks are of different robustness.

10. The method of claim 8 in which the two watermarks are encoded in accordance with different code signals.

11. A method of marking printer output from a personal computer system to permit its later identification, the system including at least a personal computer and a separate printer, the method comprising:

receiving printer data being sent from the computer to the printer;

encoding the printer data with a machine readable, steganographic digital watermark comprising a plural bit binary data, said digital watermark serving to mark the printer data as having been printed by said printer;

wherein a document printed by said printer bears said digital watermark, permitting the printer on which said document was printed to be identified, and wherein the watermark is locally adapted to the image data.

12. A method of marking printer output from a personal computer system to permit its later identification, the system including at least a personal computer and a separate printer, the method comprising:

receiving printer data being sent from the computer to the printer;

encoding the printer data with a machine readable, steganographic digital watermark comprising a plural bit binary data, said digital watermark serving to mark the printer data as having been printed by said printer;

wherein a document printed by said printer bears said digital watermark, permitting the printer on which said

20

document was printed to be identified, and wherein the watermark changes printer data luminance, not chrominance.

13. A method of marking printer output from a personal computer system to permit its later identification, the system including at least a personal computer and a separate printer, the method comprising:

receiving printer data being sent from the computer to the printer;

encoding the printer data with a machine readable, steganographic digital watermark comprising a plural bit binary data, said digital watermark serving to mark the printer data as having been printed by said printer;

wherein a document printed by said printer bears said digital watermark, permitting the printer on which said document was printed to be identified, and wherein the watermark varies values of a majority of pixels represented by the printer data.

14. A method of marking printer output from a personal computer system to permit its later identification, the system including at least a personal computer and a separate printer, the method comprising:

receiving printer data being sent from the computer to the printer;

encoding the printer data with a machine readable, steganographic digital watermark comprising a plural bit binary data, said digital watermark serving to mark the printer data as having been printed by said printer;

wherein a document printed by said printer bears said digital watermark, permitting the printer on which said document was printed to be identified, and wherein the watermark is manifested differently in different portions of the printer data.

15. A method of marking printer output from a personal computer system to permit its later identification, the system including at least a personal computer and a separate printer, the method comprising:

receiving printer data being sent from the computer to the printer;

encoding the printer data with a machine readable, steganographic digital watermark comprising a plural bit binary data, said digital watermark serving to mark the printer data as having been printed by said printer;

wherein a document printed by said printer bears said digital watermark, permitting the printer on which said document was printed to be identified, and wherein the intensity of the watermark varies with location in the printer data.

16. A method of marking printer output from a personal computer system to permit its later identification, the system including at least a personal computer and a separate printer, the method comprising:

receiving printer data being sent from the computer to the printer;

encoding the printer data with a machine readable, steganographic digital watermark comprising a plural bit binary data, said digital watermark serving to mark the printer data as having been printed by said printer;

wherein a document printed by said printer bears said digital watermark, permitting the printer on which said document was printed to be identified, and wherein the watermark changes certain pixels represented by the printer data in accordance with more than one bit of the plural bit data.



21

17. A method of image processing, comprising:  
providing image data corresponding to an optically  
scanned document to a processing apparatus; and

digitally watermarking the image data with a machine  
readable, steganographic digital watermark represent-  
ing plural bit binary data, said digital watermark serv-  
ing to mark the image data as having been processed on  
said apparatus, said watermark locally changing the  
luminance, but not the chrominance, of the image data;  
wherein said image data thereafter carries said digital  
watermark embedded therein, permitting the apparatus  
on which said image data was processed to be identi-  
fied.

18. A method of image processing, comprising:  
providing image data corresponding to an optically  
scanned document to a processing apparatus; and

digitally watermarking the image data with a machine  
readable, steganographic digital watermark represent-  
ing plural bit binary data, said digital watermark serv-  
ing to mark the image data as having been processed on  
said apparatus, said watermark altering a majority of  
pixels comprising said image data;

wherein said image data thereafter carries said digital  
watermark embedded therein, permitting the apparatus  
on which said image data was processed to be identi-  
fied.

19. A method of image processing, comprising:  
providing image data corresponding to an optically  
scanned document to a processing apparatus; and

digitally watermarking the image data with a machine  
readable, steganographic digital watermark represent-  
ing plural bit binary data, said digital watermark serv-  
ing to mark the image data as having been processed on  
said apparatus, said watermark being manifested dif-  
ferently at different regions of the image;

wherein said image data thereafter carries said digital  
watermark embedded therein, permitting the apparatus  
on which said image data was processed to be identi-  
fied.

20. A method of image processing, comprising:  
providing image data corresponding to an optically  
scanned document to a processing apparatus; and

digitally watermarking the image data with a machine  
readable, steganographic digital watermark represent-  
ing plural bit binary data, said digital watermark serv-  
ing to mark the image data as having been processed on

22

said apparatus, said watermark changing certain pixels  
of the image in accordance with more than one bit of  
said plural bit binary data;

wherein said image data thereafter carries said digital  
watermark embedded therein, permitting the apparatus  
on which said image data was processed to be identi-  
fied.

21. A method of marking scanner data provided from a  
scanner unit to a separate computer system to permit later  
identification of the scanner unit, the method comprising in  
the scanner unit:

generating first scan data;  
encoding the first scan data with a steganographic digital  
watermark representing plural bit binary data to yield  
second scan data; and

providing said second scan data from the scanner unit to  
the computer system; wherein the digital watermark in  
the second scan data serves to identify the scanner from  
which the scan data was generated—irrespective of the  
computer with which it is used.

22. The method of claim 21 wherein the watermark is  
image-adapted.

23. The method of claim 21 wherein the watermark  
changes scan data luminance, not chrominance.

24. The method of claim 21 wherein the watermark varies  
values of a majority of pixels represented by the scan data.

25. The method of claim 21 wherein the watermark is  
manifested differently in different portions of the scan data.

26. The method of claim 21 wherein the intensity of the  
watermark varies with location.

27. The method of claim 21 wherein the watermark  
changes certain pixels represented in the scan data in ac-  
cordance with more than one bit of the plural bit data.

28. The method of claim 21 wherein the watermark is not  
identifiable from human scrutiny of an image corresponding  
to the second scan data.

29. A scanner, for attachment to a separate computer, the  
scanner including plural image-sensing elements for gener-  
ating initial scan data from a paper document, the scanner  
further including a processor for digitally watermarking the  
initial scan data with a steganographic digital watermark  
conveying plural bit binary data, thereby yielding processed  
scan data for transmission to the computer, wherein said  
processed scan data conveys the digital watermark, permit-  
ting the scanner to thereafter be identified—irrespective of  
the computer with which it is used.

\* \* \* \* \*